KOREAN PATENT ABSTRACTS(KR)

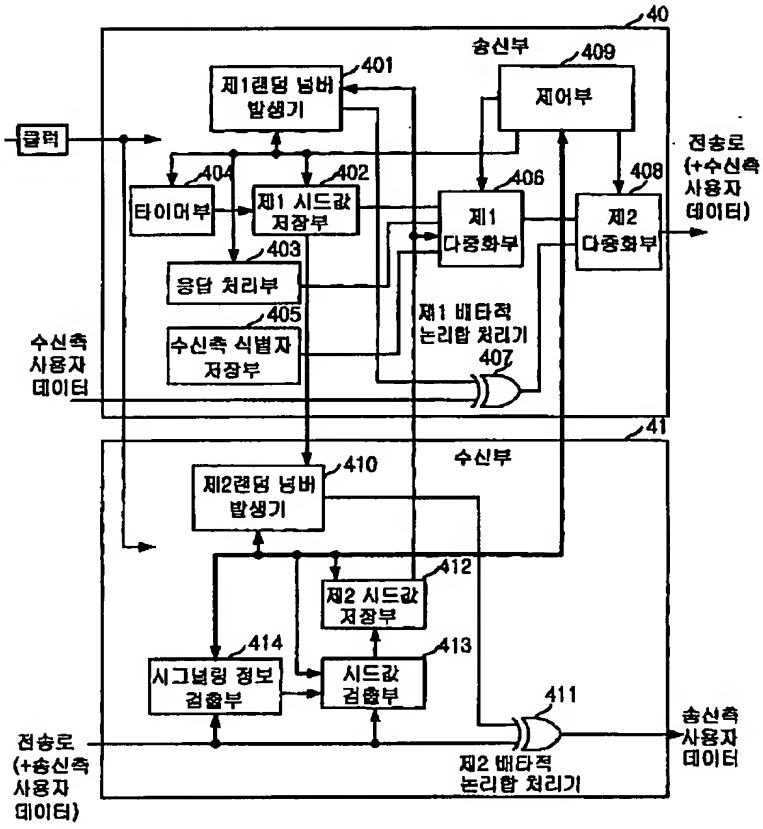
Document Code:A
(11) Publication No.1020010064800 (43) Publication.Date. 20010711
(21) Application No.1019990059090 (22) Application Date. 19991218
(51) IPC Code:
H04L 9/12

(71) Applicant:
KOREA TELECOM
(72) Inventor:
KIM, SI JUNG
LEE, JI HUN

(30) Priority:

(54) Title of Invention
APPARATUS AND METHOD FOR PROTECTING INFORMATION OF COMMUNICATION NETWORK USER

Representative drawing



(57) Abstract:

PURPOSE: An apparatus and a method for protecting information of a communication network user are provided which generates information at terminals of receiving and transmitting sides to transmit the information to a counterpart as a basic value for encoding and encodes transmission data using the basic value.

CONSTITUTION: An apparatus for protecting information of a communication network user includes a transmitter information processor and a receiver information processor. The transmitter information processor sends a signaling signal to a receiver(41) to request communication, delivers transmitter seed information obtained using a point of time of operation to the receiver,

decodes data sent from the receiver using the transmitter seed information, and accepts receiver seed information to encode transmitter user data to send it to the receiver. The receiver information processor generates a response signal to the signaling signal, encodes transmission data using the transmitter seed information, obtains the receiver seed information on the basis of the point of time of operation to send it to a transmitter(40), and decodes the data delivered from the transmitter using the receiver seed information.

IPC-Code	H04L 9/12				
Application No.	1019990059090	Application Date	19991218	Doc Kind	A
Unexamined Pub No.	1020010064800	Unexamined Pub Date	20010711		
Title of Invention	APPARATUS AND METHOD FOR PROTECTING INFORMATION OF COMMUNICATION NETWORK USER				
Priorty Country		Priorty No.		Priorty Date	

Applicant

Seq	Name
1	KOREA TELECOM

Inventor

Seq	Name
1	KIM, SI JUNG
2	LEE, JI HUN

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04L 9/12

(11) 공개번호 특2001-0064800
(43) 공개일자 2001년07월11일

(21) 출원번호 10-1999-0059090
(22) 출원일자 1999년12월18일

(71) 출원인 한국전기통신공사
경기 성남시 분당구 정자동 206

(72) 발명자 김시중
서울특별시서초구우면동17번지

이지훈
서울특별시서초구우면동17번지

(74) 대리인 특허법인 신성 박해천, 특허법인 신성 원석희, 특허법인 신성 최종식, 특허법인 신성 박정후, 특허법인 신성 정지원

심사청구 : 없음

(54) 통신망 사용자의 정보 보호 장치 및 그 방법

요약

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 통신망 사용자의 정보 보호 장치 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 교환기나 전화, 팩스 등의 사용자 터미널을 통해 데이터를 전송할 때 터미널의 이용이 시작되는 시점을 활용하여 수신측과 송신측의 터미널에서 임의 정보를 발생시켜 상대측으로 암호화를 위한 기본 값으로 전송하고 이를 사용하여 전송 데이터를 암호화하는 통신망 사용자의 정보 보호 장치 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하고자 함.

3. 발명의 해결방법의 요지

본 발명은, 시그널링 신호를 수신측으로 보내어 통신을 요청하고, 동작시점을 이용하여 얻은 송신측 시드 정보를 수신측으로 전송하고 수신측으로부터 전송된 데이터를 상기 송신측 시드 정보를 사용하여 복호화하며, 수신측 시드 정보를 전달받아 송신측 사용자 데이터를 암호화하여 수신측으로 전송하기 위한 송신측 정보 처리수단; 및 상기 송신측 정보 처리수단으로부터 전달받은 시그널링 신호에 대한 응답신호를 생성 전송하고, 전달받은 상기 송신측 시드 정보를 이용하여 전송 데이터를 암호화하며, 동작시점을 기준으로 상기 수신측 시드 정보를 얻어 송신측으로 전달하고, 송신측으로부터 전달된 데이터를 상기 수신측 시드 정보를 사용하여 복호화하기 위한 수신측 정보 처리수단을 포함함.

4. 발명의 중요한 용도

본 발명은 통신 시스템 등에 이용됨.

대표도

도4a

색인어

정보 보호, 통신, 송신측 시드 값, 수신측 시드 값, 동작시점

명세서

도면의 간단한 설명

도 1 은 종래의 통신시스템에 대한 구성예시도.

도 2 는 본 발명이 적용되는 사용자 데이터 암호화·장치의 구성예시도.

도 3 은 본 발명이 적용되는 통신시스템의 구성예시도.

도 4a 는 본 발명에 따른 수신측 통신망 사용자의 정보 보호 장치에 대한 일실시예 구성도.

도 4b 는 본 발명에 따른 수신측 통신망 사용자의 정보 보호 장치에서의 전송 신호의 일실시예 설명도.

도 5a 는 본 발명에 따른 송신측 통신망 사용자의 정보 보호 장치에 대한 일실시예 구성도.

도 5b 는 본 발명에 따른 송신측 통신망 사용자의 정보 보호 장치에서의 전송 신호의 일실시예 설명도.

도 6 은 본 발명에 따른 통신망 사용자의 정보 보호 장치에 적용되는 정보 보호 방법에 대한 일실시예 신호 흐름도.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 통신망 사용자의 정보 보호 장치 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것으로, 특히 사용자가 교환기나 사용자 터미널(전화, 팩스 등등)을 통하여 사용자 정보를 전송할 때 임의의 제 3 자에 의해서 사용자 정보가 고의적으로 감청 또는 도청되는 것을 방지하는 정보 보호 장치 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

도 1 은 종래의 통신시스템에 대한 구성예시도이다.

도 1 은 종래 사용자가 교환기나 사용자 터미널(전화, 팩스 등등)을 통해서 정보를 전달 하는 경로를 도시한 것이다.

통신시스템은, 전화기(11, 15), 교환기(12, 14) 및 통신망(13)으로 이루어져 전화기(11, 15)간에 통신이 연결되게 된다.

도 1 에 도시한 바와 같이 종래의 통신망에서는 제 3자에 의한 고의적인 감청 및 도청에 취약하게 구성이 되어있는 문제점이 있었다. 즉, 도청자는 임의의 위치에서 사용자 정보의 감시가 가능하였으며 이의 유용도 쉽게 이루어지고 있는 문제점이 있었다.

발명이 이루고자하는 기술적 과제

본 발명은 상기한 바와 같은 문제점을 해결하기 위하여 안출된 것으로, 교환기나 전화, 팩스 등의 사용자 터미널을 통해 데이터를 전송할 때 터미널의 이용이 시작되는 시점을 활용하여 수신측과 송신측의 터미널에서 임의 정보를 발생시켜 상대측으로 암호화를 위한 기본 값으로 전송하고 이를 사용하여 전송 데이터를 암호화하는 통신망 사용자의 정보 보호 장치 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위한 본 발명의 장치는, 통신망 사용자의 정보 보호 장치에 있어서, 시그널링 신호를 수신측으로 보내어 통신을 요청하고, 동작시점을 이용하여 얻은 송신측 시드 정보를 수신측으로 전송하고 수신측으로부터 전송된 데이터를 상기 송신측 시드 정보를 사용하여 복호화하며, 수신측 시드 정보를 전달받아 송신측 사용자 데이터를 암호화하여 수신측으로 전송하기 위한 송신측 정보 처리수단; 및 상기 송신측 정보 처리수단으로부터 전달받은 시그널링 신호에 대한 응답신호를 생성 전송하고, 전달받은 상기 송신측 시드 정보를 이용하여 전송 데이터를 암호화하며, 동작시점을 기준으로 상기 수신측 시드 정보를 얻어 송신측으로 전달하고, 송신측으로부터 전달된 데이터를 상기 수신측 시드 정보를 사용하여 복호화하기 위한 수신측 정보 처리수단을 포함하는 것을 특징으로 한다.

또한, 본 발명의 방법은, 통신망 사용자의 정보 보호 장치에 적용되는 통신망 사용자의 정보 보호 방법에 있어서, 수신측과의 통신연결 및 정보 보호의 통신을 위해 송신측에서 시그널링 신호와 동작시점을 기준으로 하는 송신측 시드 정보를 생성하여 수신측으로 전송하는 제 1 단계; 송신측의 통신 연결 요청에 대한 응답으로 수신측으로부터 응답신호, 수신측 식별자, 수신측의 동작시점을 기준으로 하는 수신측 시드 정보를 전송받고 상기 송신측 시드 정보를 재전송받는 제 2 단계; 재전송된 상기 송신측 시드 정보를 확인하고 전달받은 상기 수신측 시드 정보 및 송신측 전달 데이터를 상기 수신측 시드 정보로 암호화하여 수신측으로 전송하는 제 3 단계; 및 상기 수신측으로부터 전달된 데이터를 상기 송신측 시드 정보를 이용하여 복호화하는 제 4 단계를 포함하는 것을 특징으로 한다.

또한, 본 발명은, 대용량 프로세서를 구비한 통신망 사용자의 정보 보호 장치에, 수신측과의 통신연결

및 정보 보호의 통신을 위해 송신측에서 시그널링 신호와 동작시점을 기준으로 하는 송신측 시드 정보를 생성하여 수신측으로 전송하는 제 1 기능; 송신측의 통신 연결 요청에 대한 응답으로 수신측으로부터 응답신호, 수신측 식별자, 수신측의 동작시점을 기준으로 하는 수신측 시드 정보를 전송받고 상기 송신측 시드 정보를 재전송받는 제 2 기능; 재전송된 상기 송신측 시드 정보를 확인하고 전달받은 상기 수신측 시드 정보 및 송신측 전달 데이터를 상기 수신측 시드 정보로 암호화하여 수신측으로 전송하는 제 3 기능; 및 상기 수신측으로부터 전달된 데이터를 상기 송신측 시드 정보를 이용하여 복호화하는 제 4 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

본 발명은 통신망을 통하여 사용자 정보를 전송함에 있어서 발생할 수 있는 정보의 유출, 도청 등 다양한 방법에 의해서 제3자에 의한 사용자 정보의 도용을 막기 위한 기술이다.

상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

도 2 는 본 발명이 적용되는 사용자 데이터 암호화 장치의 구성예시도이다.

본 발명에서 제시하고자 하는 사용자 데이터 암호화를 위한 기능 블록도는 도 2 와 같다. 즉, 도 2 에서 전송측 및 수신측이 비슷한 기능의 암호화 블록을 갖는 터미널을 사용하는 장치로, 사용자 터미널(21)과 교환기(22)로 이루어지며, 사용자측 통신부(21)는 암호화/역암호화 처리부(212) 및 전화기(211)를 포함하여 이루어진다.

사용자 정보의 도청을 위한 위치는 교환기 또는 송신측 터미널과 수신측 터미널 사이의 임의의 위치에서 발생할 수 있다. 그러나, 본 발명은 타이머의 동작에 의한 임의의 위치에서 발생되는 시드 값을 기준으로 양측에서 암호화된 사용자 데이터를 발생, 전송함으로 제3자에 의한 정보 유출은 어렵게 된다. 도 2 의 블록도를 이용한 전체 송수신 통신시스템의 구성은 도 3 과 같이 이루어질 수 있다. 즉 암호화/역암호화 블록은 사용자 터미널에 위치할 수 있다:

도 3 은 본 발명이 적용되는 통신시스템의 구성예시도이다.

발신자가 사용자 터미널(31)에 위치하는 전화기(311)를 이용하여 통신을 할 때 암호화/역암호화 처리부(312)의 처리를 통해 암호화를 수행하여 송신측 교환기(32)와 통신망(33)을 통해 전송하고, 수신측 교환기(34)를 거쳐 수신측 터미널(35)에 도달한 전송 데이터는 수신측의 암호화/역암호화 처리부(351)를 거쳐 역암호화되어 수신측 전화기(352)를 이용하는 수신자에게 도달하게 된다.

도 4a 는 본 발명에 따른 수신측 통신망 사용자의 정보 보호 장치에 대한 일실시예 구성도이다.

본 발명에 따른 정보 보호 장치의 일실시예 수신측 구성도는 도 4 와 같다. 수신측 정보 보호 장치의 구성도의 구성은 크게 2부분으로 나뉜다. 수신측 사용자 데이터를 암호화(스크램블)하여 전송로로 전송하기 위한 전송부(40)와 송신측 사용자 데이터를 역암호화(De-scramble : 디스크램블)하여 원래의 송신측 사용자 정보로 복원하는 수신부(41)로 구성된다.

송신부(40)는 암호화 처리를 위하여 제1 랜덤넘버 발생기(401)의 시드 값 발생을 위한 타이머부(404), 제1 시드 값 저장부(402), 전송로로부터 입력되는 시그널링 정보를 처리하기 위한 응답(Ack. : Acknowledge) 처리부(403), 제1 랜덤넘버 발생기(401), 수신측 식별자(ID)를 저장하는 수신측 식별자 저장부(405), 시드 값과 응답(Ack.) 처리 데이터 및 수신측 식별자(ID), 송신측 시드 값을 다중화하는 제1 다중화부(Multiplexer1, 406), 제1 다중화부(406)의 다중화 결과와 수신측 사용자 데이터의 다중화를 위한 제2 다중화부(Multiplexer2, 408), 제1 랜덤넘버 발생기(401)의 결과와 수신측 사용자 정보를 사용하여 암호화하여 전송로로 전송하는 배타적 논리합(XOR) 처리기(407) 및 전체 블록 제어를 위한 제어부(409)를 포함하여 구성된다.

수신부(41)는 송신부(40)의 역 과정으로 전송로를 통하여 수신되는 전송측 정보의 처리를 위한 시그널링 정보 검출부(Signaling Information Detector, 414), 시드 값 검출부(413), 제2 시드 값 저장부(412) 및 제2 랜덤넘버 발생기(410), 제2 랜덤넘버 발생기(410)의 결과와 암호화된 송신측 사용자 정보를 역암호화하여 원래의 송신측 사용자 정보를 복구하는 제2 배타적 논리합(XOR) 처리기(411)를 포함하여 구성된다.

송신부(40)는 송신측 사용자 또는 교환기의 요구에 따라서 수신측 시그널링 정보(응답(Ack.) 신호 및 시드 값) 및 수신측 사용자 정보를 전송하게 된다. 먼저 수신부(41)의 시그널링 정보 검출부(414)가 전송로를 통해서 입력된 송신측 시그널링 정보를 인식하고 이를 제어부(409)에 알린다. 그리고, 시드 검출부(413)가 전송측 암호화 시드 값을 검출하여 제2 시드 값 저장부(412)에 저장한다.

제어부(409)에서는 전화기의 후크(Hook) 등의 동작에 따라서 응답(Ack.) 처리부(403)로 하여금 응답(Ack.) 신호를 발생하게 하고, 항시 동작중인 타이머(404)의 임의의 시간 위치에서의 값을 제1 시드 값 저장부(402)로 로드(Load)하게 한다.

제2 시드 값 저장부(412)에 저장되는 시드 값은 수신측이 사용자 정보를 보낼 때 암호화를 위한 제1 랜덤넘버 발생기(401)의 초기 값으로 사용된다. 그리고, 수신측에서는 더 이상 응답(Ack.) 신호, 식별자(ID) 및 수신측 시드 값을 보내지 않고, 수신측 사용자 정보를 제1 랜덤넘버 발생기(401) 결과와 제1 배타적 논리합(XOR) 처리기(407)로 암호화한 후 다중화를 위한 제2 다중화부(408)를 통과시켜 전송로로 전송하게 된다. 이때, 제1 랜덤넘버 발생기(401)의 초기 값으로는 제2 시드 값 저장부(412)에 저장된 송신측 시드 값을 사용한다.

제1 다중화부(406)는 수신측 시드 값, 수신측 식별자(ID), 응답(Ack.) 신호 및 송신측 암호화 시드 값을 다중화하고, 제2 다중화부(408)는 제1 다중화부(406)의 결과 값과 암호화된 수신측 사용자 데이터를 다중화한다.

송신부(40)에서 발생하는 신호의 전송하는 예를 아래에 설명하는 도 4b 에 도시하였다. 다중화를 위한

다중화부(406, 408)의 제어는 제어부(409)의 제어를 따르게 된다.

수신부(41)는 전송로를 통해서 입력되는 송신측 시그널링 정보를 인식하고 이를 제어부(409)에 알리게 된다. 즉 시그널링 정보 검출기(414)는 송신측 정보를 검출하여 제어부(409) 및 시드 값 검출부(413)로 하여금 응답(Ack.) 신호 발생 및 전송측 시드 값을 검출하여 제2 시드 값 저장부(412)로 저장하게 된다.

제2 시드 값 저장부(412)에 저장된 시드 값은 수신측 사용자 정보를 암호화하기 위한 랜덤넘버 발생기의 초기 값이 되며, 또한 송신부(40)의 제1 랜덤넘버발생기(401)의 시드 값이 된다.

수신측 시드 값에 의해서 초기화된 제2 랜덤넘버 발생기(410)의 결과와 전송로로부터 입력되는 암호화된 송신측 사용자 정보는 제2 배타적 논리합(XOR) 처리기(411)를 거쳐 역암호화되어 원래의 송신측 사용자 정보를 복구하게 된다

도 4b 는 본 발명에 따른 수신측 통신망 사용자의 정보 보호 장치에서의 전송 신호의 일실시예 설명도이다.

수신측 정보 보호 장치에서 전송되는 신호는 응답 시그널링 정보(Ack Signaling Information, 455), 식별자(ID, 454), 수신측 시드 값(Receiver Seed, 453), 송신측 시드 값(Transmitter Seed, 452) 및 사용자 데이터(User Data, 451) 등으로 송신측 정보 보호 장치에서 이를 수신하게 된다.

도 5a 는 본 발명에 따른 송신측 통신망 사용자의 정보 보호 장치에 대한 일실시예 구성도이다.

도 5를 기준으로 송신측 암호화 블록도의 구성 및 작용을 기술한다. 송신측 암호화 블록도의 구성은 크게 2부분으로 구성된다.

송신측 사용자 데이터를 암호화(스크램블)하여 전송로로 전송하기 위한 전송부(51)와 수신측 사용자 데이터를 역암호화(De-scramble : 디스크램블)하여 원래의 수신자 정보로 복원하는 수신부(52)로 구성된다. 송신부(51)는 암호화 처리를 위하여 랜덤넘버발생기의 시드 값 발생을 위한 타이머부(521), 제1 시드 값 저장부(516), 제어부(514)의 제어에 의해서 시그널링 정보를 발생하는 시그널링 정보 처리부(520), 제1 랜덤넘버발생기(515), 시드 값과 시그널링 데이터를 다중화하는 제1 다중화부(Multiplexer, 517), 시드 정보 및 시그널링 데이터와 전송부 사용자 데이터의 다중화를 위한 제2 다중화부(Multiplexer, 519), 제1 랜덤넘버발생기(515)의 결과를 이용하여 전송측 사용자 데이터를 암호화하는 제1 배타적 논리합 처리기(XOR, 518) 및 전체 블록의 제어를 위한 제어부(514)로 구성되고, 수신부(52)는 전송부(51)의 역과정 처리를 하게 되며 전송로를 통하여 수신되는 수신측 정보 처리를 위한 응답(Ack.) 처리부(526), 수신측 랜덤넘버발생기의 기본 값이 되는 시드 값 검출부(524), 시드 값 검출부(524)의 결과를 저장하는 시드 값 저장부(523), 제2 랜덤넘버발생기(522), 시드 값 저장부 및 랜덤넘버발생기의 결과를 이용하여 수신측 사용자 데이터를 역암호화하는 제2 배타적 논리합 처리기(525)로 구성된다.

전송부(51)는 전송측 사용자의 요구에 따라서 사용자 정보 전송을 위한 시그널링 정보를 발생한다. 즉, 제어부(514)에서 시그널링 정보 처리부(520)로 하여금 시그널링 정보를 발생하도록 하여 전송로로 보내게 된다. 이때 제어부(514)에서는 항시 동작중인 타이머(521)의 임의의 위치에서의 값을 제1 시드 값 저장부(516)로 로드(Load)하게 한다. 이 값은 수신측 사용자 데이터를 암호화하는 랜덤넘버발생기의 시드 값으로 사용되며 수신측 사용자 데이터는 이 결과 값으로 암호화된다. 또한 전송측 수신부는 이 값을 랜덤넘버발생기(22)의 기본 값으로 사용하고 암호화된 수신측 사용자 데이터의 복구를 위하여 사용된다. 수신측에서 이 값의 사용을 위하여 전송측 송신부에서는 두 개의 먹스(17, 19)로 시간적인 다중화를 거쳐 시그널링 정보 바로 뒤에 붙여서 하기의 도 5b 에 도시된 송신측 전송 신호와 같이 송신하게 된다.

그리고, 수신측의 응답으로 전송되는 신호를 수신부(52)의 응답(Ack.) 처리부(526)가 처리하여 수신측에서 정확히 전송부(51)의 시그널링 정보와 전송측 시드 값을 받았다는 것을 확인하고 이를 제어부(514)에 알린다. 제어부(514)는 더 이상 시그널링 정보를 보내지 않고 수신측에서 보낸 시드 값이 현재 암호화에 사용중인 수신측 시드 값과의 확인을 위하여 수신측 시드 값을 재전송하고, 또한, 송신측 사용자 데이터를 수신측 시드 값을 기본으로 하는 제1 랜덤넘버발생기(515) 결과 값과 제1 배타적 논리합 처리기(18)로 암호화한 후 다중화를 위한 제2 다중화부(519)를 통과 시켜 전송로로 전송하게 된다. 도 5b 에 송신측 전송신호를 도시하였다.

수신부(52)는 전송부(51)의 시그널링 정보 전송 결과 수신측으로부터 전송되는 데이터를 처리하게 된다.

먼저, 응답(Ack.) 처리부(526)는 수신측이 정확히 송신측의 시그널링 정보와 시드 값을 받았다는 것을 확인하는 정보를 인식하고, 그 결과를 제어부(514)에 통보한다. 그리고, 시드 값 검출부(524)로 하여금 전송로 상의 수신측 암호화 시드 값을 확인하게 하고, 이를 시드 값 저장부(23)로 저장하게 한다.

또한, 응답(Ack.) 처리부(526)는 송신측과 수신측이 고정된 시드 값을 사용하는 암호화 시스템에서 수신측 사용자의 식별자(ID) 값을 수신하여 제어부(514)에 알리게 된다. 제어부(514)에서는 송신측 사용자 정보를 전송할 때 이 식별자(ID)에 맞는 시드 값을 제1 랜덤넘버발생기(515)의 초기 값으로 사용한다. 제어부(514)는 시드 값을 제2 시드 값 저장부(523)에 저장하도록 하고, 제1 랜덤넘버발생기(515)는 이 시드 값을 기본으로 난수를 발생하게 되며, 제1 랜덤넘버발생기(515)의 결과를 이용하여 송신측 사용자 데이터를 제1 배타적 논리합 처리기(518)에서 암호화하게 된다. 송신측 시드 값을 기본 값으로 사용하는 제2 랜덤넘버발생기(522)는 전송로로 입력되는 암호화된 수신측 사용자 정보를 제2 배타적 논리합 처리기(525)를 거쳐 역 암호화함으로 원래의 수신측 사용자 데이터를 복구하게 된다.

도 5b 는 본 발명에 따른 송신측 통신망 사용자의 정보 보호 장치에서의 전송 신호의 일실시예 설명도이다.

송신측에서 전송하는 신호는 시그널링 정보(Signalling Information, 554), 송신측 시드값(Transmitter Seed, 553), 수신측 시드값(Receiver Seed, 552) 및 사용자 데이터(User Data, 551) 등으로 수신측에서

이를 수신하게 된다.

도 6 은 본 발명에 따른 통신망 사용자의 정보 보호 장치에 적용되는 정보 보호 방법에 대한 일실시예 신호 흐름도이다.

도 6 에서는 송신측 및 수신측 신호 흐름을 도시하였다. 그림에서 보는 것과 같이 신호의 흐름은 다음과 같다.

우선, 송신측 시그널링 정보 및 수신측 사용자 데이터의 암호화를 위해 사용되는 송신측 시드 값 정보를 송신측 정보 보호 장치에서 수신측 정보 보호 장치로 전송한다(601).

수신측 정보 보호 장치에서 수신측 응답(Ack.) 신호와 수신측 식별자(Id), 송신측 사용자 데이터의 암호화를 위해 사용되는 수신측 시드 값 정보 및 송신측으로부터 수신하여 수신측의 사용자 데이터 암호화에 사용할 송신측 시드 값 정보를 송신측 정보 보호 장치로 전송한다(602).

수신측 정보 보호 장치는 송신측 시드 값을 수신측 사용자 데이터의 암호화에 사용하도록 설정하고, 전송받은 송신측 시드 값이 송신측 정보 보호 장치에서 보낸 원래의 송신측 시드 값과 같은지를 확인하기 위해 재전송하게 된다.

송신측 정보 보호 장치에서 송신측 사용자 데이터의 암호화를 위해 사용되는 수신측 정보 보호 장치로부터 수신한 수신측 시드 값 정보 및 수신측 시드 값을 사용하여 암호화된 송신측 사용자 데이터를 수신측 정보 보호 장치로 전송한다(603).

송신측 정보 보호 장치는 수신측 시드 값을 송신측 사용자 데이터의 암호화에 사용하도록 설정하고, 전송받은 수신측 시드 값이 수신측 정보 보호 장치에서 보낸 원래의 수신측 시드 값과 같은지를 확인하기 위해 재전송하게 되며, 재전송받은 송신측 시드 값에 대하여는 원래의 송신측 시드 값과 같은지를 확인한다. 확인 결과, 이상이 있으면 송신측 시드 값을 다시 보내게 된다.

수신측 정보 보호 장치에서는 송신측 시드값으로 암호화한 수신측 사용자 데이터를 송신측 정보 보호 장치로 전송한다(604).

수신측 정보 보호 장치는 재전송받은 수신측 시드 값에 대하여 원래의 수신측 시드 값과 같은지를 확인한다. 확인 결과, 이상이 있으면 수신측 시드 값을 다시 보내게 된다.

송신측 정보 보호 장치는 수신측 정보 보호 장치와의 데이터 전달이 끝나 송신측 호 종료를 수신측으로 전달한다(605).

수신측 정보 보호 장치도 송신측 정보 보호 장치와의 데이터 전달이 끝나 수신측 호 종료를 송신측으로 전달한다(606).

이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다.

발명의 효과

상기한 바와 같은 본 발명은, 사용자가 교환기나 사용자 터미널(전화, 팩스 등등)을 통하여 사용자 정보를 전송할 때 착신자가 수신측 터미널을 사용하기 시작한 시점을 이용하여 수신측 터미널에서 임의 정보를 발생시켜 발신자 측으로 전달하여 암호화를 위한 기본값으로 이용하도록 하고, 수신측 터미널의 암호화를 위한 기본값으로는 송신측의 동작 시점을 이용하여 송신측 터미널에서 임의 정보를 발생시켜 얻은 값을 사용하여 사용자 데이터를 보호함으로써 제 3자에 의한 고의적인 사용자 데이터의 감청이나 도청을 방지할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1

통신망 사용자의 정보 보호 장치에 있어서,

시그널링 신호를 수신측으로 보내어 통신을 요청하고, 동작시점을 이용하여 얻은 송신측 시드 정보를 수신측으로 전송하고 수신측으로부터 전송된 데이터를 상기 송신측 시드 정보를 사용하여 복호화하며, 수신측 시드 정보를 전달받아 송신측 사용자 데이터를 암호화하여 수신측으로 전송하기 위한 송신측 정보 처리수단: 및

상기 송신측 정보 처리수단으로부터 전달받은 시그널링 신호에 대한 응답신호를 생성 전송하고, 전달받은 상기 송신측 시드 정보를 이용하여 전송 데이터를 암호화하며, 동작시점을 기준으로 상기 수신측 시드 정보를 얻어 송신측으로 전달하고, 송신측으로부터 전달된 데이터를 상기 수신측 시드 정보를 사용하여 복호화하기 위한 수신측 정보 처리수단

을 포함하는 통신망 사용자의 정보 보호 장치.

청구항 2

제 1 항에 있어서,

상기 송신측 정보 처리수단은,

상기 수신측 정보 처리수단으로 상기 시그널링 신호, 상기 송신측 시드 정보, 상기 수신측 시드 정보로 암호화된 송신측 사용자 데이터 등을 만들어 전송하기 위한 송신측 전송 처리수단; 및

상기 수신측 정보 처리수단으로부터 상기 응답신호, 수신측 식별자, 상기 수신측 시드 정보, 상기 송신측 시드 정보로 암호화된 수신측 사용자 데이터 등을 수신하여 처리하기 위한 송신측 수신 처리수단

을 포함하는 통신망 사용자의 정보 보호 장치.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 수신측 정보 처리수단은,

상기 송신측 정보 처리수단으로 상기 응답신호, 상기 수신측 식별자, 상기 수신측 시드 정보, 상기 송신측 시드 정보로 암호화된 수신측 사용자 데이터 등을 생성하여 전송하기 위한 수신측 전송 처리수단; 및

상기 송신측 정보 처리수단으로부터 상기 시그널링 신호, 상기 송신측 시드 정보, 상기 수신측 시드 정보로 암호화된 송신측 사용자 데이터 등을 수신하여 처리하기 위한 송신측 수신 처리수단

을 포함하는 통신망 사용자의 정보 보호 장치.

청구항 4

통신망 사용자의 정보 보호 장치에 적용되는 통신망 사용자의 정보 보호 방법에 있어서,

수신측과의 통신연결 및 정보 보호의 통신을 위해 송신측에서 시그널링 신호와 동작시점을 기준으로 하는 송신측 시드 정보를 생성하여 수신측으로 전송하는 제 1 단계;

송신측의 통신 연결 요청에 대한 응답으로 수신측으로부터 응답신호, 수신측 식별자, 수신측의 동작시점을 기준으로 하는 수신측 시드 정보를 전송받고 상기 송신측 시드 정보를 재전송받는 제 2 단계;

재전송된 상기 송신측 시드 정보를 확인하고 전달받은 상기 수신측 시드 정보 및 송신측 전달 데이터를 상기 수신측 시드 정보로 암호화하여 수신측으로 전송하는 제 3 단계; 및

상기 수신측으로부터 전달된 데이터를 상기 송신측 시드 정보를 이용하여 복호화하는 제 4 단계

를 포함하는 통신망 사용자의 정보 보호 방법.

청구항 5

제 4 항에 있어서,

상기 수신측과의 통신 연결을 종료하기 위해 호 종료 요청 신호를 전송하고 이에 대한 응답으로 호 종료 응답 신호를 전달받아 통신 연결을 종료하는 제 5 단계

를 더 포함하는 통신망 사용자의 정보 보호 방법.

청구항 6

제 4 항에 있어서,

상기 수신측으로부터 통신 연결 종료를 위한 호 종료 요청 신호를 전달받아 이에 대한 응답으로 호 종료 응답 신호를 전송하여 통신 연결을 종료하는 제 5 단계

를 더 포함하는 통신망 사용자의 정보 보호 방법.

청구항 7

대용량 프로세서를 구비한 통신망 사용자의 정보 보호 장치에,

수신측과의 통신연결 및 정보 보호의 통신을 위해 송신측에서 시그널링 신호와 동작시점을 기준으로 하는 송신측 시드 정보를 생성하여 수신측으로 전송하는 제 1 기능;

송신측의 통신 연결 요청에 대한 응답으로 수신측으로부터 응답신호, 수신측 식별자, 수신측의 동작시점을 기준으로 하는 수신측 시드 정보를 전송받고 상기 송신측 시드 정보를 재전송받는 제 2 기능;

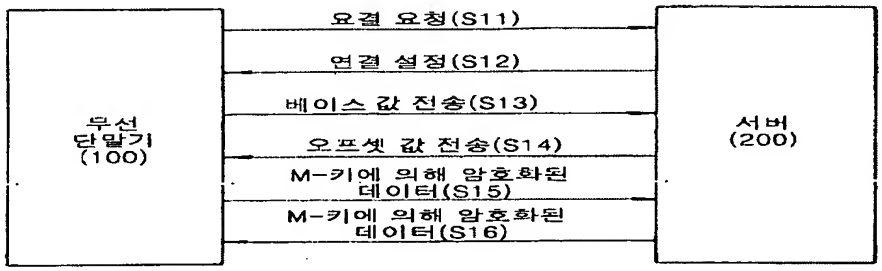
재전송된 상기 송신측 시드 정보를 확인하고 전달받은 상기 수신측 시드 정보 및 송신측 전달 데이터를 상기 수신측 시드 정보로 암호화하여 수신측으로 전송하는 제 3 기능; 및

상기 수신측으로부터 전달된 데이터를 상기 송신측 시드 정보를 이용하여 복호화하는 제 4 기능

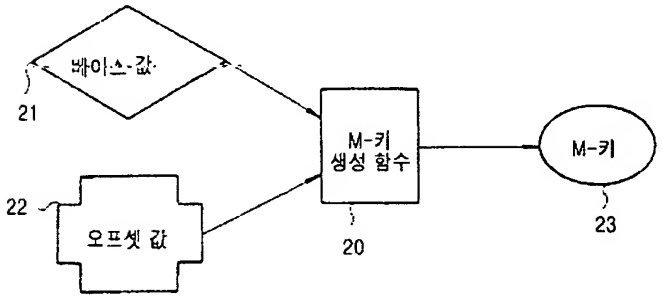
을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

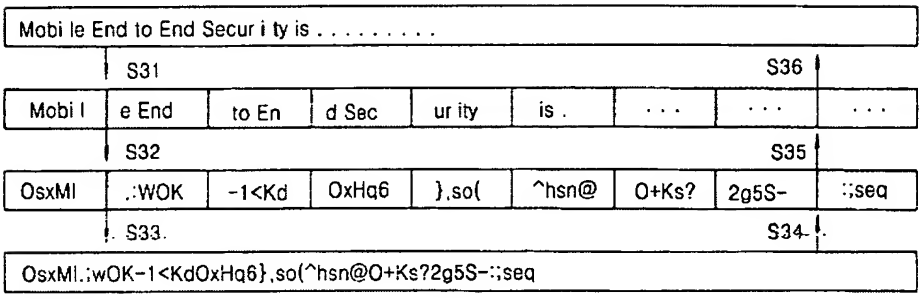
도면1



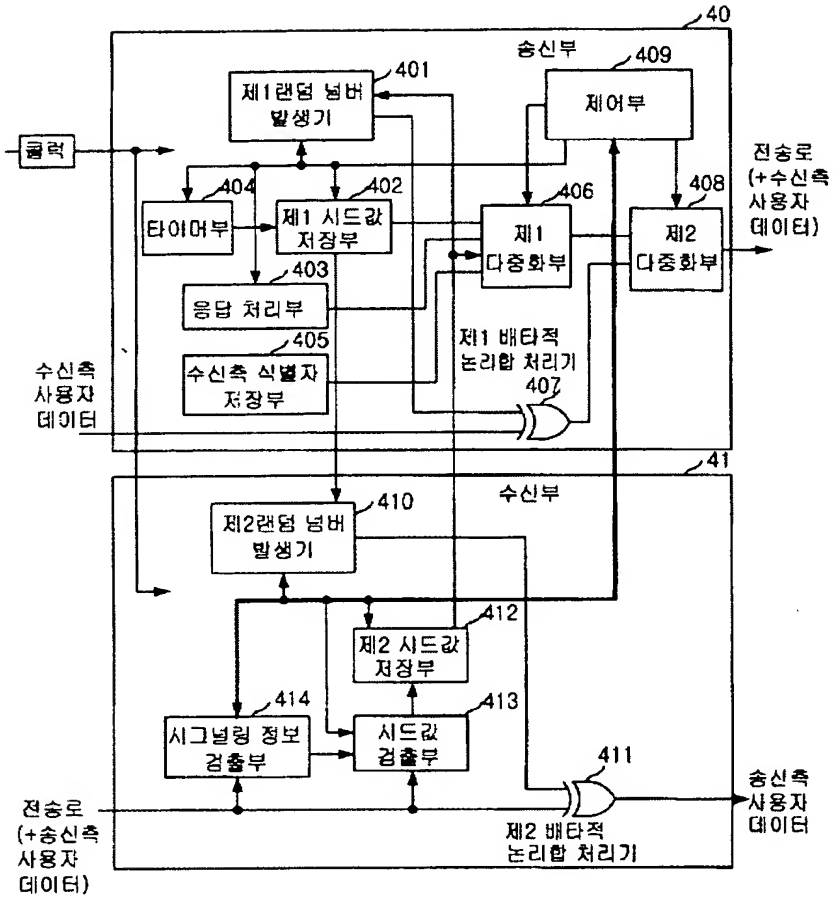
도면2



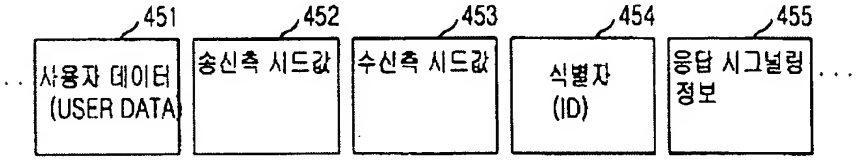
도면3



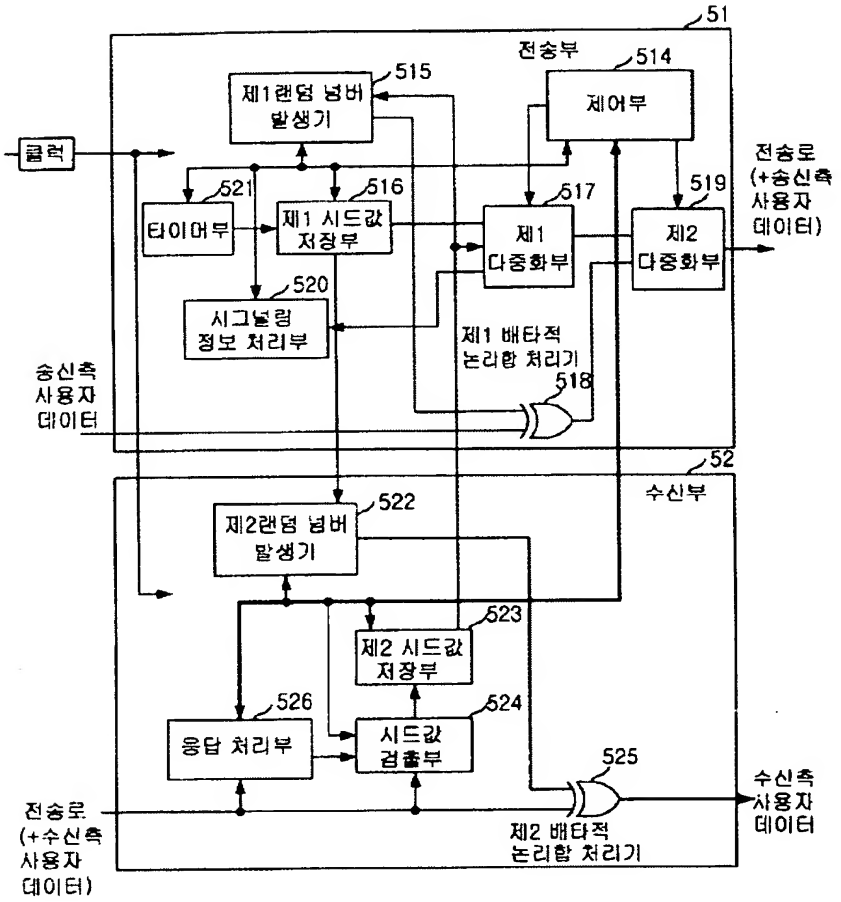
도면4a


40
송신부
409
제어부
401
제1랜덤 넘버 발생기
입력
전송로 (+수신측 사용자 데이터)
404
402
406
408
타이머부
제1 시드값 저장부
제1 다중화부
제2 다중화부
403
응답 처리부
405
수신측 식별자 저장부
제1 배타적 논리합 처리기
407
수신측 사용자 데이터
41
수신부
410
제2랜덤 넘버 발생기
412
제2 시드값 저장부
414
413
시그널링 정보 검출부
시드값 검출부
411
송신측 사용자 데이터
전송로 (+송신측 사용자 데이터)
제2 배타적 논리합 처리기

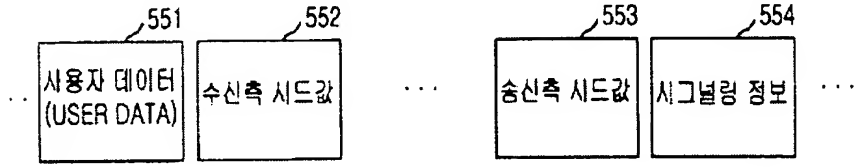
도면4b


451
452
453
454
455
사용자 데이터 (USER DATA)
송신측 시드값
수신측 시드값
식별자 (ID)
응답 시그널링 정보

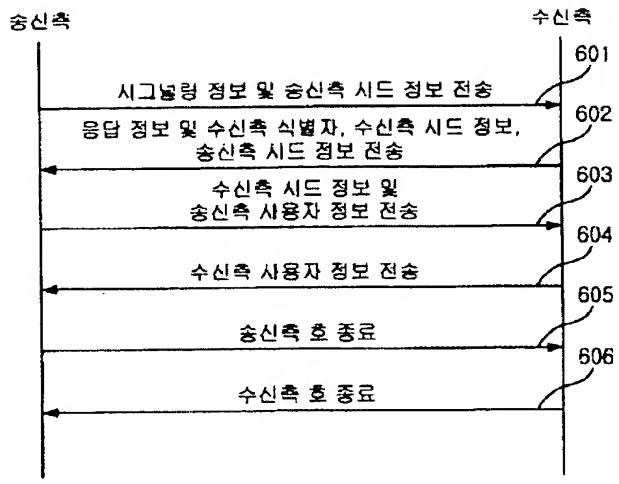
도면5a


51
전송부
514
제어부
515
제1랜덤 넘버 발생기
클럭
521
타이머부
516
제1 시드값 저장부
517
제1 다중화부
519
제2 다중화부
전송로 (+송신측 사용자 데이터)
520
시그널링 정보 처리부
제1 배타적 논리합 처리기
518
송신측 사용자 데이터
52
수신부
522
제2랜덤 넘버 발생기
523
제2 시드값 저장부
526
응답 처리부
524
시드값 검출부
525
수신측 사용자 데이터
전송로 (+수신측 사용자 데이터)
제2 배타적 논리합 처리기

도면5b


551
552
553
554
사용자 데이터 (USER DATA)
수신측 시드값
송신측 시드값
시그널링 정보

도면6


송신측
수신측
601
시그널링 정보 및 송신측 시드 정보 전송
602
응답 정보 및 수신측 식별자, 수신측 시드 정보,
송신측 시드 정보 전송
603
수신측 시드 정보 및
송신측 사용자 정보 전송
604
수신측 사용자 정보 전송
605
송신측 호 종료
606
수신측 호 종료